

AN ACT Relating to the management, oversight, and use of data; adding new chapters to Title 19 RCW; adding a new chapter to Title 43 RCW; adding a new section to chapter 42.56 RCW; prescribing penalties; and providing an effective date.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF WASHINGTON:

1 NEW SECTION. **Sec. 1.** SHORT TITLE. This act may be known and
2 cited as the Washington privacy act.

3 NEW SECTION. **Sec. 2.** LEGISLATIVE FINDINGS AND INTENT. (1) The
4 legislature finds that the people of Washington regard their privacy
5 as a fundamental right and an essential element of their individual
6 freedom. Washington's Constitution explicitly provides the right to
7 privacy, and fundamental privacy rights have long been and continue
8 to be integral to protecting Washingtonians and to safeguarding our
9 democratic republic.

10 (2) Ongoing advances in technology have produced an exponential
11 growth in the volume and variety of personal data being generated,

1 collected, stored, and analyzed, which presents both promise and
2 potential peril. The ability to harness and use data in positive
3 ways is driving innovation and brings beneficial technologies to
4 society; however, it has also created risks to privacy and freedom.
5 The unregulated and unauthorized use and disclosure of personal
6 information and loss of privacy can have devastating impacts,
7 ranging from financial fraud, identity theft, and unnecessary costs,
8 to personal time and finances, to destruction of property,
9 harassment, reputational damage, emotional distress, and physical
10 harm.

11 (3) Given that technological innovation and new uses of data can
12 help solve societal problems, protect public health associated with
13 global pandemics, and improve quality of life, the legislature seeks
14 to shape responsible public policies where innovation and protection
15 of individual privacy coexist. The legislature notes that our
16 federal authorities have not developed or adopted into law
17 regulatory or legislative solutions that give consumers control over
18 their privacy. In contrast, the European Union's general data
19 protection regulation has continued to influence data privacy
20 policies and practices of those businesses competing in global
21 markets. In the absence of federal standards, Washington and other
22 states across the United States are analyzing elements of the
23 European Union's general data protection regulation to enact state-
24 based data privacy regulatory protections.

25 (4) Responding to COVID-19 illustrates the need for public
26 policies that protect individual privacy while fostering
27 technological innovation. For years, contact tracing best practices
28 have been used by public health officials to securely process high
29 value individual data and have effectively stopped the prolific
30 spread of infectious diseases. However, the scale of COVID-19 is
31 unprecedented. Contact tracing is evolving in a manner that
32 necessitates the use of technology to rapidly collect and process
33 data from multiple data sets, many of which are unanticipated, to

1 protect public health as well as to facilitate the continued safe
2 operation of the economy. The benefits of such technology, however,
3 should not supersede the potential privacy risks to individuals.

4 (5) Exposure notification applications have already been
5 deployed throughout the country and the world; however, contact
6 tracing technology is rapidly evolving. Applications may be
7 integrated in a manner that facilitates the aggregation and sharing
8 of individual data that in effect generate profiles of individuals.
9 Artificial intelligence may be used for the extrapolation of data to
10 analyze and interpret data for public health purposes. Moreover, the
11 potential government use of exposure notification applications poses
12 additional potential privacy risks to individuals due to the types
13 of sensitive data it has access to and processes. Much of that
14 processing may have legal effects, including access to services or
15 establishments. The capabilities of next generation contact tracing
16 technologies are unknown and policies must be in place to provide
17 privacy protections for current uses as well as potential future
18 uses.

19 (6) With this act, the legislature intends to provide a modern
20 privacy regulatory framework with data privacy guardrails to protect
21 individual privacy; to instill public confidence on the processing
22 use of their personal and public health data during any global
23 pandemic; and to require companies to be responsible custodians of
24 data as technological innovations emerge.

25 (7) This act gives consumers the ability to protect their own
26 rights to privacy by explicitly providing consumers the right to
27 access, correction, and deletion of personal data, as well as the
28 right to opt out of the collection and use of personal data for
29 certain purposes. These rights will add to, and not subtract from,
30 the consumer protection rights that consumers already have under
31 Washington state law.

32 (7) This act also imposes affirmative obligations upon companies
33 to safeguard personal data, and provide clear, understandable, and

1 transparent information to consumers about how their personal data
2 are used. It strengthens compliance and accountability by requiring
3 data protection assessments in the collection and use of personal
4 data. Finally, it empowers the state attorney general to obtain and
5 evaluate a company's data protection assessments, to impose
6 penalties where violations occur, and to prevent against future
7 violations.

8 (9) The legislature also encourages the state office of privacy
9 and data protection to monitor the development of universal privacy
10 controls that communicate a consumer's affirmative, freely given,
11 and unambiguous choice to opt out of the processing of personal data
12 concerning the consumer for the purposes of targeted advertising,
13 the sale of personal data, or profiling in furtherance of decisions
14 that produce legal effects concerning the consumer or similarly
15 significant effects concerning consumers.

16 **PART 1**

17 **Personal Data Privacy Regulations - Private Sector**

18 NEW SECTION. **Sec. 101.** DEFINITIONS. The definitions in this
19 section apply throughout this chapter unless the context clearly
20 requires otherwise.

21 (1) "Affiliate" means a legal entity that controls, is
22 controlled by, or is under common control with, that other legal
23 entity. For these purposes, "control" or "controlled" means
24 ownership of, or the power to vote, more than fifty percent of the
25 outstanding shares of any class of voting security of a company;
26 control in any manner over the election of a majority of the
27 directors or of individuals exercising similar functions; or the
28 power to exercise a controlling influence over the management of a
29 company.

30 (2) "Authenticate" means to use reasonable means to determine
31 that a request to exercise any of the rights in section 103 (1)
32 through (4) of this act is being made by the consumer who is

1 entitled to exercise such rights with respect to the personal data
2 at issue.

3 (3) "Business associate" has the same meaning as in Title 45
4 C.F.R., established pursuant to the federal health insurance
5 portability and accountability act of 1996.

6 (4) "Child" means any natural person under thirteen years of
7 age.

8 (5) "Consent" means a clear affirmative act signifying a freely
9 given, specific, informed, and unambiguous indication of a
10 consumer's agreement to the processing of personal data relating to
11 the consumer, such as by a written statement, including by
12 electronic means, or other clear affirmative action.

13 (6) "Consumer" means a natural person who is a Washington
14 resident acting only in an individual or household context. It does
15 not include a natural person acting in a commercial or employment
16 context.

17 (7) "Controller" means the natural or legal person which, alone
18 or jointly with others, determines the purposes and means of the
19 processing of personal data.

20 (8) "Covered entity" has the same meaning as in Title 45 C.F.R.,
21 established pursuant to the federal health insurance portability and
22 accountability act of 1996.

23 (9) "Decisions that produce legal effects concerning a consumer
24 or similarly significant effects concerning a consumer" means
25 decisions that result in the provision or denial of financial and
26 lending services, housing, insurance, education enrollment, criminal
27 justice, employment opportunities, health care services, or access
28 to basic necessities, such as food and water.

29 (10) "Deidentified data" means data that cannot reasonably be
30 used to infer information about, or otherwise be linked to, an
31 identified or identifiable natural person, or a device linked to
32 such person, provided that the controller that possesses the data:

33 (a) Takes reasonable measures to ensure that the data cannot be

1 associated with a natural person; (b) publicly commits to maintain
2 and use the data only in a deidentified fashion and not attempt to
3 reidentify the data; and (c) contractually obligates any recipients
4 of the information to comply with all provisions of this subsection.

5 (11) "Health care facility" has the same meaning as in RCW
6 70.02.010.

7 (12) "Health care information" has the same meaning as in RCW
8 70.02.010.

9 (13) "Health care provider" has the same meaning as in RCW
10 70.02.010.

11 (14) "Identified or identifiable natural person" means a person
12 who can be readily identified, directly or indirectly.

13 (15) "Institutions of higher education" has the same meaning as
14 in RCW 28B.92.030.

15 (16) "Legislative agencies" has the same meaning as in RCW
16 44.80.020.

17 (17) "Local government" has the same meaning as in RCW
18 39.46.020.

19 (18) "Nonprofit corporation" has the same meaning as in RCW
20 24.03.005.

21 (19)(a) "Personal data" means any information that is linked or
22 reasonably linkable to an identified or identifiable natural person.
23 "Personal data" does not include deidentified data or publicly
24 available information.

25 (b) For purposes of this subsection, "publicly available
26 information" means information that is lawfully made available from
27 federal, state, or local government records.

28 (20) "Process" or "processing" means any operation or set of
29 operations which are performed on personal data or on sets of
30 personal data, whether or not by automated means, such as the
31 collection, use, storage, disclosure, analysis, deletion, or
32 modification of personal data.

1 (21) "Processor" means a natural or legal person who processes
2 personal data on behalf of a controller.

3 (22) "Profiling" means any form of automated processing of
4 personal data to evaluate, analyze, or predict personal aspects
5 concerning an identified or identifiable natural person's economic
6 situation, health, personal preferences, interests, reliability,
7 behavior, location, or movements.

8 (23) "Protected health information" has the same meaning as in
9 Title 45 C.F.R., established pursuant to the federal health
10 insurance portability and accountability act of 1996.

11 (24) "Pseudonymous data" means personal data that cannot be
12 attributed to a specific natural person without the use of
13 additional information, provided that such additional information is
14 kept separately and is subject to appropriate technical and
15 organizational measures to ensure that the personal data are not
16 attributed to an identified or identifiable natural person.

17 (25)(a) "Sale," "sell," or "sold" means the exchange of personal
18 data for monetary or other valuable consideration by the controller
19 to a third party.

20 (b) "Sale" does not include the following: (i) The disclosure of
21 personal data to a processor who processes the personal data on
22 behalf of the controller; (ii) the disclosure of personal data to a
23 third party with whom the consumer has a direct relationship for
24 purposes of providing a product or service requested by the
25 consumer; (iii) the disclosure or transfer of personal data to an
26 affiliate of the controller; (iv) the disclosure of information that
27 the consumer (A) intentionally made available to the general public
28 via a channel of mass media, and (B) did not restrict to a specific
29 audience; or (v) the disclosure or transfer of personal data to a
30 third party as an asset that is part of a merger, acquisition,
31 bankruptcy, or other transaction in which the third party assumes
32 control of all or part of the controller's assets.

1 (26) "Security or safety purpose" means physical security,
2 protection of consumer data, safety, fraud prevention, or asset
3 protection.

4 (27) "Sensitive data" means (a) personal data revealing racial
5 or ethnic origin, religious beliefs, mental or physical health
6 condition or diagnosis, sexual orientation, or citizenship or
7 immigration status; (b) the processing of genetic or biometric data
8 for the purpose of uniquely identifying a natural person; (c) the
9 personal data from a known child; or (d) specific geolocation data.
10 "Sensitive data" is a form of personal data.

11 (28) "Specific geolocation data" means information derived from
12 technology, including, but not limited to, global positioning system
13 level latitude and longitude coordinates or other mechanisms, that
14 directly identifies the specific location of a natural person with
15 the precision and accuracy below one thousand seven hundred fifty
16 feet. Specific geolocation data excludes the content of
17 communications.

18 (29) "State agency" has the same meaning as in RCW 43.105.020.

19 (30) "Targeted advertising" means displaying advertisements to a
20 consumer where the advertisement is selected based on personal data
21 obtained from a consumer's activities over time and across
22 nonaffiliated web sites or online applications to predict such
23 consumer's preferences or interests. It does not include
24 advertising: (a) Based on activities within a controller's own web
25 sites or online applications; (b) based on the context of a
26 consumer's current search query or visit to a web site or online
27 application; or (c) to an individual in response to the consumer's
28 request for information or feedback.

29 (31) "Third party" means a natural or legal person, public
30 authority, agency, or body other than the consumer, controller,
31 processor, or an affiliate of the processor or the controller.

1 NEW SECTION. **Sec. 102.** JURISDICTIONAL SCOPE. (1) This chapter
2 applies to legal entities that conduct business in Washington or
3 produce products or services that are targeted to residents of
4 Washington, and that satisfy one or more of the following
5 thresholds:

6 (a) During a calendar year, controls or processes personal data
7 of one hundred thousand consumers or more; or

8 (b) Derives over twenty-five percent of gross revenue from the
9 sale of personal data and processes or controls personal data of
10 twenty-five thousand consumers or more.

11 (2) This chapter does not apply to:

12 (a) State agencies, legislative agencies, local governments,
13 tribes;

14 (b) Nonprofit corporations;

15 (c) Institutions of higher education;

16 (d) Municipal corporations;

17 (e) Information that meets the definition of:

18 (i) Protected health information for purposes of the federal
19 health insurance portability and accountability act of 1996 and
20 related regulations;

21 (ii) Health care information for purposes of chapter 70.02 RCW;

22 (iii) Patient identifying information for purposes of 42 C.F.R.
23 Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;

24 (iv) Identifiable private information for purposes of the
25 federal policy for the protection of human subjects, 45 C.F.R. Part
26 46; identifiable private information that is otherwise information
27 collected as part of human subjects research pursuant to the good
28 clinical practice guidelines issued by the international council for
29 harmonisation; the protection of human subjects under 21 C.F.R.
30 Parts 50 and 56; or personal data used or shared in research
31 conducted in accordance with one or more of the requirements set
32 forth in this subsection;

1 (v) Information and documents created specifically for, and
2 collected and maintained by:

3 (A) A quality improvement committee for purposes of RCW
4 43.70.510, 70.230.080, or 70.41.200;

5 (B) A peer review committee for purposes of RCW 4.24.250;

6 (C) A quality assurance committee for purposes of RCW 74.42.640
7 or 18.20.390;

8 (D) A hospital, as defined in RCW 43.70.056, for reporting of
9 health care-associated infections for purposes of RCW 43.70.056, a
10 notification of an incident for purposes of RCW 70.56.040(5), or
11 reports regarding adverse events for purposes of RCW
12 70.56.020(2)(b);

13 (vi) Information and documents created for purposes of the
14 federal health care quality improvement act of 1986, and related
15 regulations;

16 (vii) Patient safety work product for purposes of 42 C.F.R. Part
17 3, established pursuant to 42 U.S.C. Sec. 299b-21 through 299b-26;
18 or

19 (viii) Information that is (A) deidentified in accordance with
20 the requirements for deidentification set forth in 45 C.F.R. Part
21 164, and (B) derived from any of the health care-related information
22 listed in this subsection (2)(e);

23 (f) Information originating from, and intermingled to be
24 indistinguishable with, information under (e) of this subsection
25 that is maintained by:

26 (i) A covered entity or business associate as defined by the
27 health insurance portability and accountability act of 1996 and
28 related regulations;

29 (ii) A health care facility or health care provider as defined
30 in RCW 70.02.010; or

31 (iii) A program or a qualified service organization as defined
32 by 42 C.F.R. Part 2, established pursuant to 42 U.S.C. Sec. 290dd-2;

1 (g) Information used only for public health activities and
2 purposes as described in 45 C.F.R. Sec. 164.512;

3 (h)(i) An activity involving the collection, maintenance,
4 disclosure, sale, communication, or use of any personal information
5 bearing on a consumer's credit worthiness, credit standing, credit
6 capacity, character, general reputation, personal characteristics,
7 or mode of living by a consumer reporting agency, as defined in
8 Title 15 U.S.C. Sec. 1681a(f), by a furnisher of information, as set
9 forth in Title 15 U.S.C. Sec. 1681s-2, who provides information for
10 use in a consumer report, as defined in Title 15 U.S.C. Sec.
11 1681a(d), and by a user of a consumer report, as set forth in Title
12 15 U.S.C. Sec. 1681b.

13 (ii) (f)(i) of this subsection shall apply only to the extent
14 that such activity involving the collection, maintenance,
15 disclosure, sale, communication, or use of such information by that
16 agency, furnisher, or user is subject to regulation under the fair
17 credit reporting act, Title 15 U.S.C. Sec. 1681 et seq., and the
18 information is not collected, maintained, used, communicated,
19 disclosed, or sold except as authorized by the fair credit reporting
20 act;

21 (i) Personal data collected and maintained for purposes of
22 chapter 43.71 RCW;

23 (j) Personal data collected, processed, sold, or disclosed
24 pursuant to the federal Gramm-Leach-Bliley act (P.L. 106-102), and
25 implementing regulations, if the collection, processing, sale, or
26 disclosure is in compliance with that law;

27 (k) Personal data collected, processed, sold, or disclosed
28 pursuant to the federal driver's privacy protection act of 1994 (18
29 U.S.C. Sec. 2721 et seq.), if the collection, processing, sale, or
30 disclosure is in compliance with that law;

31 (l) Personal data regulated by the federal family education
32 rights and privacy act, 20 U.S.C. Sec. 1232g and its implementing
33 regulations;

1 (m) Personal data regulated by the student user privacy in
2 education rights act, chapter 28A.604 RCW;

3 (n) Personal data collected, processed, sold, or disclosed
4 pursuant to the federal farm credit act of 1971 (as amended in 12
5 U.S.C. Sec. 2001-2279cc) and its implementing regulations (12 C.F.R.
6 Part 600 et seq.) if the collection, processing, sale, or disclosure
7 is in compliance with that law; or

8 (o) Data maintained for employment records purposes.

9 (3) Controllers that are in compliance with the verifiable
10 parental consent mechanisms under the children's online privacy
11 protection act, Title 15 U.S.C. Sec. 6501 through 6506 and its
12 implementing regulations, shall be deemed compliant with any
13 obligation to obtain parental consent under this chapter.

14 (4) Payment-only credit, check, or cash transactions where no
15 data about consumers are retained do not count as " consumers" for
16 purposes of subsection (1) of this section.

17 NEW SECTION. **Sec. 103.** CONSUMER RIGHTS. (1) *Access.* A consumer
18 has the right to confirm whether or not a controller is processing
19 personal data concerning the consumer and access such personal data.

20 (2) *Correction.* A consumer has the right to correct inaccurate
21 personal data concerning the consumer, taking into account the
22 nature of the personal data and the purposes of the processing of
23 the personal data.

24 (3) *Deletion.* A consumer has the right to delete personal data
25 concerning the consumer.

26 (4) *Data portability.* A consumer has the right to obtain
27 personal data concerning the consumer, which the consumer previously
28 provided to the controller, in a portable and, to the extent
29 technically feasible, readily usable format that allows the
30 individual to transmit the data to another controller without
31 hindrance, where the processing is carried out by automated means.

1 (5) *Opt out of certain processing.* A consumer has the right to
2 opt out of the processing of personal data concerning such consumer
3 for purposes of targeted advertising, the sale of personal data, or
4 profiling in furtherance of decisions that produce legal effects
5 concerning a consumer or similarly significant effects concerning a
6 consumer.

7 NEW SECTION. **Sec. 104.** EXERCISING CONSUMER RIGHTS. (1)
8 Consumers may exercise the rights set forth in section 103 of this
9 chapter by submitting a request, at any time, to a controller
10 specifying which rights the individual wishes to exercise.

11 (2) In the case of processing personal data concerning a known
12 child, the parent or legal guardian of the known child shall
13 exercise the rights of this chapter on the child's behalf.

14 (3) In the case of processing personal data concerning a
15 consumer subject to guardianship, conservatorship, or other
16 protective arrangement under chapter 11.88 RCW, chapter 11.92 RCW,
17 or chapter 11.130 RCW, the guardian or the conservator of the
18 consumer shall exercise the rights of this chapter on the consumer's
19 behalf.

20
21 NEW SECTION. **Sec. 105.** RESPONDING TO REQUESTS. (1) Except as
22 provided in this chapter, the controller must comply with a request
23 to exercise the rights pursuant to section 103 of this act.

24 (2)(a) Controllers must provide one or more secure and reliable
25 means for consumers to submit a request to exercise their rights
26 under this chapter. Such means shall take into account the ways in
27 which consumers interact with the controller and the need for secure
28 and reliable communication of such requests.

29 (b) Controllers shall not require a consumer to create a new
30 account in order to exercise a right, but a controller may require a
31 consumer to use an existing account to exercise the consumer's
32 rights under this chapter.

1 (3)(a) A controller must inform a consumer of any action taken
2 on a request under section 104 of this act without undue delay and
3 in any event within forty-five days of receipt of the request. That
4 period may be extended once by forty-five additional days where
5 reasonably necessary, taking into account the complexity and number
6 of the requests. The controller must inform the consumer of any such
7 extension within forty-five days of receipt of the request, together
8 with the reasons for the delay.

9 (b) If a controller does not take action on the request of a
10 consumer, the controller must inform the consumer without undue
11 delay and at the latest within forty-five days of receipt of the
12 request of the reasons for not taking action and instructions for
13 how to appeal the decision with the controller as described in
14 subsection (3) of this section.

15 (c) Information provided under this section must be provided by
16 the controller free of charge, up to twice annually to the consumer.
17 Where requests from a consumer are manifestly unfounded or
18 excessive, in particular because of their repetitive character, the
19 controller may either: (i) Charge a reasonable fee to cover the
20 administrative costs of complying with the request, or (ii) refuse
21 to act on the request. The controller bears the burden of
22 demonstrating the manifestly unfounded or excessive character of the
23 request.

24 (d) A controller is not required to comply with a request to
25 exercise any of the rights under subsections (1) through (4) of
26 section 103 of this act if the controller is unable to authenticate
27 the request using commercially reasonable efforts. In such cases,
28 the controller may request the provision of additional information
29 reasonably necessary to authenticate the request.

30 (4)(a) Controllers must establish an internal process whereby
31 consumers may appeal a refusal to take action on a request to
32 exercise any of the rights under section 103 of this act within a

1 reasonable period of time after the consumer's receipt of the notice
2 sent by the controller under subsection (3)(b) of this section.

3 (b) The appeal process must be conspicuously available and as
4 easy to use as the process for submitting such requests under this
5 section.

6 (c) Within thirty days of receipt of an appeal, a controller
7 must inform the consumer of any action taken or not taken in
8 response to the appeal, along with a written explanation of the
9 reasons in support thereof. That period may be extended by sixty
10 additional days where reasonably necessary, taking into account the
11 complexity and number of the requests serving as the basis for the
12 appeal. The controller must inform the consumer of any such
13 extension within thirty days of receipt of the appeal, together with
14 the reasons for the delay. The controller must also provide the
15 consumer with an email address or other online mechanism through
16 which the consumer may submit the appeal, along with any action
17 taken or not taken by the controller in response to the appeal and
18 the controller's written explanation of the reasons in support
19 thereof, to the attorney general.

20 (d) When informing a consumer of any action taken or not taken
21 in response to an appeal pursuant to (c) of this subsection, the
22 controller must clearly and prominently ask the consumer whether the
23 consumer consents to having the controller submit the appeal, along
24 with any action taken or not taken by the controller in response to
25 the appeal and must, upon request, provide the controller's written
26 explanation of the reasons in support thereof, to the attorney
27 general. If the consumer provides such consent, the controller must
28 submit such information to the attorney general.

29 NEW SECTION. **Sec. 106.** RESPONSIBILITY ACCORDING TO ROLE. (1)
30 Controllers and processors are responsible for meeting their
31 respective obligations established under this chapter.

1 (2) Processors are responsible under this chapter for adhering
2 to the instructions of the controller and assisting the controller
3 to meet its obligations under this chapter. Such assistance shall
4 include the following:

5 (a) Taking into account the nature of the processing, the
6 processor shall assist the controller by appropriate technical and
7 organizational measures, insofar as this is possible, for the
8 fulfillment of the controller's obligation to respond to consumer
9 requests to exercise their rights pursuant to section 103 of this
10 act; and

11 (b) Taking into account the nature of processing and the
12 information available to the processor, the processor shall assist
13 the controller in meeting the controller's obligations in relation
14 to the security of processing the personal data and in relation to
15 the notification of a breach of the security of the system pursuant
16 to RCW 19.255.010; and shall provide information to the controller
17 necessary to enable the controller to conduct and document any data
18 protection assessments required by section 113 of this chapter.

19 (3) Notwithstanding the instructions of the controller, a
20 processor shall:

21 (a) Implement and maintain reasonable security procedures and
22 practices to protect personal data, taking into account the context
23 in which the personal data are to be processed;

24 (b) Ensure that each person processing the personal data is
25 subject to a duty of confidentiality with respect to the data; and

26 (c) Engage a subcontractor only after providing the controller
27 with an opportunity to object and pursuant to a written contract in
28 accordance with subsection (5) of this section that requires the
29 subcontractor to meet the obligations of the processor with respect
30 to the personal data.

31 (4) Processing by a processor shall be governed by a contract
32 between the controller and the processor that is binding on both
33 parties and that sets out the processing instructions to which the

1 processor is bound, including the nature and purpose of the
2 processing, the type of personal data subject to the processing, the
3 duration of the processing, and the obligations and rights of both
4 parties. In addition, the contract shall include the requirements
5 imposed by this subsection and subsection (3) of this section, as
6 well as the following requirements:

7 (a) At the choice of the controller, the processor shall delete
8 or return all personal data to the controller as requested at the
9 end of the provision of services, unless retention of the personal
10 data is required by law;

11 (b)(i) The processor shall make available to the controller all
12 information necessary to demonstrate compliance with the obligations
13 in this chapter; and (ii) the processor shall allow for, and
14 contribute to, reasonable audits and inspections by the controller
15 or the controller's designated auditor; alternatively, the processor
16 may, with the controller's consent, arrange for a qualified and
17 independent auditor to conduct, at least annually and at the
18 processor's expense, an audit of the processor's policies and
19 technical and organizational measures in support of the obligations
20 under this chapter using an appropriate and accepted control
21 standard or framework and audit procedure for such audits as
22 applicable, and shall provide a report of such audit to the
23 controller upon request.

24 (5) In no event shall any contract relieve a controller or a
25 processor from the liabilities imposed on them by virtue of its role
26 in the processing relationship as defined by this chapter.

27 (6) Determining whether a person is acting as a controller or
28 processor with respect to a specific processing of data is a fact-
29 based determination that depends upon the context in which personal
30 data are to be processed. A person that is not limited in its
31 processing of personal data pursuant to a controller's instructions,
32 or that fails to adhere to such instructions, is a controller and
33 not a processor with respect to a specific processing of data. A

1 processor that continues to adhere to a controller's instructions
2 with respect to a specific processing of personal data remains a
3 processor. If a processor begins, alone or jointly with others,
4 determining the purposes and means of the processing of personal
5 data, it is a controller with respect to such processing.

6 NEW SECTION. **Sec. 107.** RESPONSIBILITIES OF CONTROLLERS. (1)

7 *Transparency.* (a) Controllers shall provide consumers with a
8 reasonably accessible, clear, and meaningful privacy notice that
9 includes:

10 (i) The categories of personal data processed by the controller;

11 (ii) The purposes for which the categories of personal data are
12 processed;

13 (iii) How and where consumers may exercise the rights contained
14 in section 103 of this act, including how a consumer may appeal a
15 controller's action with regard to the consumer's request;

16 (iv) The categories of personal data that the controller shares
17 with third parties, if any; and

18 (v) The categories of third parties, if any, with whom the
19 controller shares personal data.

20 (b) If a controller sells personal data to third parties or
21 processes personal data for targeted advertising, it must clearly
22 and conspicuously disclose such processing, as well as the manner in
23 which a consumer may exercise the right to opt out of such
24 processing, in a clear and conspicuous manner.

25 (2) *Purpose specification.* A controller's collection of personal
26 data must be limited to what is reasonably necessary in relation to
27 the purposes for which such data are processed.

28 (3) *Data minimization.* A controller's collection of personal
29 data must be adequate, relevant, and limited to what is reasonably
30 necessary in relation to the purposes for which such data are
31 processed.

1 (4) *Avoid secondary use.* Except as provided in this chapter, a
2 controller may not process personal data for purposes that are not
3 reasonably necessary to, or compatible with, the purposes for which
4 such personal data are processed unless the controller obtains the
5 consumer's consent.

6 (5) *Security.* A controller shall establish, implement, and
7 maintain reasonable administrative, technical, and physical data
8 security practices to protect the confidentiality, integrity, and
9 accessibility of personal data. Such data security practices shall
10 be appropriate to the volume and nature of the personal data at
11 issue.

12 (6) *Nondiscrimination.* A controller shall not process personal
13 data on the basis of a consumer's or a class of consumers' actual or
14 perceived race, color, ethnicity, religion, national origin, sex,
15 gender, gender identity, sexual orientation, familial status, lawful
16 source of income, or disability, in a manner that unlawfully
17 discriminates against the consumer or class of consumers with
18 respect to the offering or provision of (a) housing, (b) employment,
19 (c) credit, (d) education, or (e) the goods, services, facilities,
20 privileges, advantages, or accommodations of any place of public
21 accommodation.

22 (7) *Antiretaliation.* A controller shall not discriminate against
23 a consumer for exercising any of the rights contained in this
24 chapter, including denying goods or services to the consumer,
25 charging different prices or rates for goods or services, and
26 providing a different level of quality of goods and services to the
27 consumer. This subsection shall not prohibit a controller from
28 offering a different price, rate, level, quality, or selection of
29 goods or services to a consumer, including offering goods or
30 services for no fee, if the offering is in connection with a
31 consumer's voluntary participation in a bona fide loyalty, rewards,
32 premium features, discounts, or club card program. A controller may
33 not sell personal data to a third-party controller as part of such a

1 program unless: (a) The sale is reasonably necessary to enable the
2 third party to provide a benefit to which the consumer is entitled;
3 (b) the sale of personal data to third parties is clearly disclosed
4 in the terms of the program; and (c) the third party uses the
5 personal data only for purposes of facilitating such benefit to
6 which the consumer is entitled and does not retain or otherwise use
7 or disclose the personal data for any other purpose.

8 (8) *Sensitive data*. Except as otherwise provided in this act, a
9 controller may not process sensitive data concerning a consumer
10 without obtaining the consumer's consent, or, in the case of the
11 processing of personal data concerning a known child, without
12 obtaining consent from the child's parent or lawful guardian, in
13 accordance with the children's online privacy protection act
14 requirements.

15 (9) *Nonwaiver of consumer rights*. Any provision of a contract or
16 agreement of any kind that purports to waive or limit in any way a
17 consumer's rights under this chapter shall be deemed contrary to
18 public policy and shall be void and unenforceable.

19 NEW SECTION. **Sec. 108.** PROCESSING DEIDENTIFIED DATA OR
20 PSEUDONYMOUS DATA. (1) This chapter does not require a controller
21 or processor to do any of the following solely for purposes of
22 complying with this chapter:

23 (a) Reidentify deidentified data;

24 (b) Comply with an authenticated consumer request to access,
25 correct, delete, or port personal data pursuant to section 103 (1)
26 through (4) of this act, if all of the following are true:

27 (i)(A) The controller is not reasonably capable of associating
28 the request with the personal data, or (B) it would be unreasonably
29 burdensome for the controller to associate the request with the
30 personal data;

31 (ii) The controller does not use the personal data to recognize
32 or respond to the specific consumer who is the subject of the

1 personal data, or associate the personal data with other personal
2 data about the same specific consumer; and

3 (iii) The controller does not sell the personal data to any
4 third party or otherwise voluntarily disclose the personal data to
5 any third party other than a processor, except as otherwise
6 permitted in this section; or

7 (c) Maintain data in identifiable form, or collect, obtain,
8 retain, or access any data or technology, in order to be capable of
9 associating an authenticated consumer request with personal data.

10 (2) The rights contained in section 103 (1) through (4) of this
11 act do not apply to pseudonymous data in cases where the controller
12 is able to demonstrate any information necessary to identify the
13 consumer is kept separately and is subject to effective technical
14 and organizational controls that prevent the controller from
15 accessing such information.

16 (3) A controller that uses pseudonymous data or deidentified
17 data must exercise reasonable oversight to monitor compliance with
18 any contractual commitments to which the pseudonymous data or
19 deidentified data are subject and must take appropriate steps to
20 address any breaches of contractual commitments.

21
22 NEW SECTION. **Sec. 109.** DATA PROTECTION ASSESSMENTS. (1)
23 Controllers must conduct and document a data protection assessment
24 of each of the following processing activities involving personal
25 data:

26 (a) The processing of personal data for purposes of targeted
27 advertising;

28 (b) The sale of personal data;

29 (c) The processing of personal data for purposes of profiling,
30 where such profiling presents a reasonably foreseeable risk of: (i)
31 Unfair or deceptive treatment of, or disparate impact on, consumers;
32 (ii) financial, physical, or reputational injury to consumers; (iii)
33 a physical or other intrusion upon the solitude or seclusion, or the

1 private affairs or concerns, of consumers, where such intrusion
2 would be offensive to a reasonable person; or (iv) other substantial
3 injury to consumers;

4 (d) The processing of sensitive data; and

5 (e) Any processing activities involving personal data that
6 present a heightened risk of harm to consumers.

7 Such data protection assessments must take into account the type
8 of personal data to be processed by the controller, including the
9 extent to which the personal data are sensitive data, and the
10 context in which the personal data are to be processed.

11 (2) Data protection assessments conducted under subsection (1)
12 of this section must identify and weigh the benefits that may flow
13 directly and indirectly from the processing to the controller,
14 consumer, other stakeholders, and the public against the potential
15 risks to the rights of the consumer associated with such processing,
16 as mitigated by safeguards that can be employed by the controller to
17 reduce such risks. The use of deidentified data and the reasonable
18 expectations of consumers, as well as the context of the processing
19 and the relationship between the controller and the consumer whose
20 personal data will be processed, must be factored into this
21 assessment by the controller.

22 (3) The attorney general may request, in writing, that a
23 controller disclose any data protection assessment that is relevant
24 to an investigation conducted by the attorney general. The
25 controller must make a data protection assessment available to the
26 attorney general upon such a request. The attorney general may
27 evaluate the data protection assessments for compliance with the
28 responsibilities contained in section 107 of this act and with other
29 laws including, but not limited to, chapter 19.86 RCW. Data
30 protection assessments are confidential and exempt from public
31 inspection and copying under chapter 42.56 RCW. The disclosure of a
32 data protection assessment pursuant to a request from the attorney
33 general under this subsection does not constitute a waiver of the

1 attorney-client privilege or work product protection with respect to
2 the assessment and any information contained in the assessment.

3 (4) Data protection assessments conducted by a controller for
4 the purpose of compliance with other laws or regulations may qualify
5 under this section if they have a similar scope and effect.

6 NEW SECTION. **Sec. 110.** LIMITATIONS AND APPLICABILITY. (1) The
7 obligations imposed on controllers or processors under this chapter
8 do not restrict a controller's or processor's ability to:

9 (a) Comply with federal, state, or local laws, rules, or
10 regulations;

11 (b) Comply with a civil, criminal, or regulatory inquiry,
12 investigation, subpoena, or summons by federal, state, local, or
13 other governmental authorities;

14 (c) Cooperate with law enforcement agencies concerning conduct
15 or activity that the controller or processor reasonably and in good
16 faith believes may violate federal, state, or local laws, rules, or
17 regulations;

18 (d) Investigate, establish, exercise, prepare for, or defend
19 legal claims;

20 (e) Provide a product or service specifically requested by a
21 consumer, perform a contract to which the consumer is a party, or
22 take steps at the request of the consumer prior to entering into a
23 contract;

24 (f) Take immediate steps to protect an interest that is
25 essential for the life of the consumer or of another natural person,
26 and where the processing cannot be manifestly based on another legal
27 basis;

28 (g) Prevent, detect, protect against, or respond to security
29 incidents, identity theft, fraud, harassment, malicious or deceptive
30 activities, or any illegal activity; preserve the integrity or
31 security of systems; or investigate, report, or prosecute those
32 responsible for any such action;

1 (h) Engage in public or peer-reviewed scientific, historical, or
2 statistical research in the public interest that adheres to all
3 other applicable ethics and privacy laws as long as such processing
4 is disclosed to the individual in the notice required under section
5 107 of this act; or

6 (i) Assist another controller, processor, or third party with
7 any of the obligations under this subsection.

8 (2) The obligations imposed on controllers or processors under
9 this chapter do not restrict a controller's or processor's ability
10 to collect, use, or retain data to:

11 (a) Conduct internal research solely to improve or repair
12 products, services, or technology;

13 (b) Identify and repair technical errors that impair existing or
14 intended functionality; or

15 (c) Perform solely internal operations that are reasonably
16 aligned with the expectations of the consumer based on the
17 consumer's existing relationship with the controller, or are
18 otherwise compatible with processing in furtherance of the provision
19 of a product or service specifically requested by a consumer or the
20 performance of a contract to which the consumer is a party.

21 (3) The obligations imposed on controllers or processors under
22 this chapter do not apply where compliance by the controller or
23 processor with this chapter would violate an evidentiary privilege
24 under Washington law and do not prevent a controller or processor
25 from providing personal data concerning a consumer to a person
26 covered by an evidentiary privilege under Washington law as part of
27 a privileged communication.

28 (4) A controller or processor that discloses personal data to a
29 third-party controller or processor in compliance with the
30 requirements of this chapter is not in violation of this chapter if
31 the recipient processes such personal data in violation of this
32 chapter, provided that, at the time of disclosing the personal data,
33 the disclosing controller or processor did not have actual knowledge

1 that the recipient intended to commit a violation. A third-party
2 controller or processor receiving personal data from a controller or
3 processor in compliance with the requirements of this chapter is
4 likewise not in violation of this chapter for the obligations of the
5 controller or processor from which it receives such personal data.

6 (5) Obligations imposed on controllers and processors under this
7 chapter shall not:

8 (a) Adversely affect the rights or freedoms of any persons, such
9 as exercising the right of free speech pursuant to the First
10 Amendment to the United States Constitution; or

11 (b) Apply to the processing of personal data by a natural person
12 in the course of a purely personal or household activity.

13 (6) Personal data that are processed by a controller pursuant to
14 this section must not be processed for any purpose other than those
15 expressly listed in this section. Personal data that are processed
16 by a controller pursuant to this section may be processed solely to
17 the extent that such processing is: (i) Necessary, reasonable, and
18 proportionate to the purposes listed in this section; and (ii)
19 adequate, relevant, and limited to what is necessary in relation to
20 the specific purpose or purposes listed in this section.

21 Furthermore, personal data that are collected, used, or retained
22 pursuant to subsection (2) of this section must, insofar as
23 possible, taking into account the nature and purpose or purposes of
24 such collection, use, or retention, be subjected to reasonable
25 administrative, technical, and physical measures to protect the
26 confidentiality, integrity, and accessibility of the personal data,
27 and to reduce reasonably foreseeable risks of harm to consumers
28 relating to such collection, use, or retention of personal data.

29 (7) If a controller processes personal data pursuant to an
30 exemption in subsection (1) of this section, the controller bears
31 the burden of demonstrating that such processing qualifies for the
32 exemption and complies with the requirements in subsection (6) of
33 this section.

1 (8) Processing personal data solely for the purposes expressly
2 identified in subsection (1)(a) through (d) or (g) of this section
3 does not, by itself, make an entity a controller with respect to
4 such processing.

5 NEW SECTION. **Sec. 111.** LIABILITY. (1) Any violation of this
6 chapter shall not serve as the basis for, or be subject to, a
7 private right of action under this chapter or under any other law.
8 This does not relieve any party from any duties or obligations
9 imposed, or to alter any independent rights that consumers have
10 under other laws, chapter 19.86 RCW, the Washington state
11 Constitution, or the United States Constitution.

12 (2) Where more than one controller or processor, or both a
13 controller and a processor, involved in the same processing, is in
14 violation of this chapter, the liability must be allocated among the
15 parties according to principles of comparative fault.

16 NEW SECTION. **Sec. 112.** ENFORCEMENT. (1) The legislature finds
17 that the practices covered by this chapter are matters vitally
18 affecting the public interest for the purpose of applying the
19 consumer protection act, chapter 19.86 RCW. A violation of this
20 chapter is not reasonable in relation to the development and
21 preservation of business and is an unfair or deceptive act in trade
22 or commerce and an unfair method of competition for the purpose of
23 applying the consumer protection act, chapter 19.86 RCW.

24 (2) This chapter may be enforced solely by the attorney general
25 under the consumer protection act, chapter 19.86 RCW.

26 (3) Prior to initiating any action under this act, the attorney
27 general must provide a controller thirty days' written notice
28 identifying the specific provisions of this title the attorney
29 general, on behalf of a consumer, alleges have been or are being
30 violated. In the event a cure is possible, if within the thirty days
31 the controller cures the noticed violation and provides the consumer
32 an express written statement that the violations have been cured and

1 that no further violations shall occur, no action for statutory
2 damages may be initiated against the controller. If a controller
3 continues to violate this title in breach of the express written
4 statement provided to the consumer under this subsection, the
5 attorney general may initiate an action and seek damages of up to
6 seven thousand and five hundred dollars for each violation under
7 this act.

8 (4) All receipts from the imposition of civil penalties under
9 this chapter must be deposited into the consumer privacy account
10 established in section 113 of this act.

11 NEW SECTION. **Sec. 113.** CONSUMER PRIVACY ACCOUNT. The consumer
12 privacy account is created in the state treasury. All receipts from
13 the imposition of civil penalties under this chapter must be
14 deposited into the account. Moneys in the account may be spent only
15 after appropriation. Moneys in the account may only be used for the
16 purposes of recovery of costs and attorney's fees accrued by the
17 attorney general in enforcing this chapter and for the office of
18 privacy and data protection as created under RCW 43.105.369. Moneys
19 may not be used to supplant general fund appropriations to either
20 agency.

21 NEW SECTION. **Sec. 114.** PREEMPTION. (1) Except as provided in
22 this section, this chapter supersedes and preempts laws, ordinances,
23 regulations, or the equivalent adopted by any local entity regarding
24 the processing of personal data by controllers or processors.

25 (2) Laws, ordinances, or regulations regarding the processing of
26 personal data by controllers or processors that are adopted by any
27 local entity prior to July 1, 2020, are not superseded or preempted.

28 NEW SECTION. **Sec. 115.** ATTORNEY GENERAL REPORT. (1) The
29 attorney general shall compile a report (a) evaluating the liability
30 and enforcement provisions of this chapter including, but not
31 limited to, the effectiveness of its efforts to enforce this

1 chapter, and any recommendations for changes to such provisions; and
2 (b) summarizing the data protected and not protected by this chapter
3 including, but not limited to, with reasonable detail, a list of the
4 types of information that are publicly available from local, state,
5 and federal government sources, and an inventory of information to
6 which this chapter does not apply by virtue of a limitation in
7 section 104 of this act. The attorney general may consult with the
8 office of privacy and data protection when compiling the report and
9 may update the report as new information becomes available.

10 (2) The attorney general shall submit the report to the governor
11 and the appropriate committees of the legislature by July 1, 2022.

12 NEW SECTION. **Sec. 116.** JOINT RESEARCH INITIATIVES. The
13 governor may enter into agreements with the governments of the
14 Canadian province of British Columbia and the states of California
15 and Oregon for the purpose of sharing personal data or personal
16 information by public bodies across national and state borders to
17 enable collaboration for joint data-driven research initiatives.
18 Such agreements must provide reciprocal protections that the
19 respective governments agree appropriately safeguard the data.

20 NEW SECTION. **Sec. 117.** A new section is added to chapter 42.56
21 RCW to read as follows:

22 Data protection assessments submitted by a controller to the
23 attorney general in accordance with requirements under section 109
24 of this act are exempt from disclosure under this chapter.

25 **PART 2**

26 **Data Privacy Regarding Public Health Emergency - Private Sector**

27 NEW SECTION. **Sec. 201.** The definitions in this section apply
28 throughout this chapter unless the context clearly requires
29 otherwise.

1 (1) "Authenticate" means to use reasonable means to determine
2 that a request to exercise any of the rights in section 203 of this
3 act is being made by the consumer who is entitled to exercise such
4 rights with respect to the covered data at issue.

5 (2) "Child" means any natural person under thirteen years of
6 age.

7 (3) "Consent" means a clear affirmative act signifying a freely
8 given, specific, informed, and unambiguous indication of a
9 consumer's agreement to the processing of covered data relating to
10 the consumer, such as by a written statement, including by
11 electronic means, or other clear affirmative action.

12 (4) "Consumer" means a natural person who is a Washington
13 resident acting only in an individual or household context. It does
14 not include a natural person acting in a commercial or employment
15 context.

16 (5) "Controller" means the natural or legal person which, alone
17 or jointly with others, determines the purposes and means of the
18 processing of covered data.

19 (6) "Covered data" includes personal data and one or more of the
20 following: specific geolocation data, proximity data, or personal
21 health data.

22 (7) "Covered purpose" means processing of covered data
23 concerning a consumer for the purposes of detecting symptoms of an
24 infectious disease, enabling the tracking of a consumer's contacts
25 with other consumers, or with specific locations to identify in an
26 automated fashion whom consumers have come into contact with, or
27 digitally notifying, in an automated manner, a consumer who may have
28 become exposed to an infectious disease, or other similar purposes
29 directly related to a state of emergency declared by the governor
30 pursuant to RCW 43.06.010 and any restrictions imposed under the
31 state of emergency declared by the governor pursuant to RCW
32 43.06.200 through 43.06.270.

1 (8) "Deidentified data" means data that cannot reasonably be
2 used to infer information about, or otherwise be linked to, an
3 identified or identifiable natural person, or a device linked to
4 such person, provided that the controller that possesses the data:
5 (a) Takes reasonable measures to ensure that the data cannot be
6 associated with a natural person; (b) publicly commits to maintain
7 and use the data only in a deidentified fashion and not attempt to
8 reidentify the data; and (c) contractually obligates any recipients
9 of the information to comply with all provisions of this subsection.

10 (9) "Delete" means to remove or destroy information such that it
11 is not maintained in human or machine-readable form and cannot be
12 retrieved or utilized in the course of business.

13 (10) "Identified or identifiable natural person" means a
14 consumer who can be readily identified, directly or indirectly.

15 (11)(a) "Personal data" means any information that is linked or
16 reasonably linkable or describes or is reasonably capable of being
17 associated to an identified or identifiable natural person.
18 "Personal data" does not include deidentified data or publicly
19 available information.

20 (b) For purposes of this subsection, "publicly available
21 information" means information that is lawfully made available from
22 federal, state, or local government records.

23 (12) (a) "Personal health data" means information relating to the
24 past, present, or future diagnosis or treatment of a consumer
25 regarding an infectious disease.

26 (13) "Process," "processed," or "processing" means any operation
27 or set of operations which are performed on covered data or on sets
28 of covered data by automated means, such as the collection, use,
29 storage, disclosure, analysis, deletion, or modification of covered
30 data.

31 (14) "Processor" means a natural or legal person that processes
32 covered data on behalf of a controller.

1 (15) "Proximity data" means technologically derived information
2 that identifies past or present proximity of one consumer to
3 another, or the proximity of natural persons to other locations or
4 objects.

5 (16) "Secure" means encrypted in a manner that meets or exceeds
6 the national institute of standards and technology standard or is
7 otherwise modified so that the covered data is rendered unreadable,
8 unusable, or undecipherable by an unauthorized person.

9 (17) "Sell" means the exchange of covered data for monetary or
10 other valuable consideration by the controller to a third party.

11 (18) "Specific geolocation data" means information derived from
12 technology, including, but not limited to, global positioning system
13 level latitude and longitude coordinates or other mechanisms, that
14 directly identifies the specific location of a natural person with
15 the precision and accuracy below one thousand seven hundred fifty
16 feet. Specific geolocation data excludes the content of
17 communications.

18 (19) "Third party" means a natural or legal person, public
19 authority, agency, or body other than the consumer, controller,
20 processor, or an affiliate of the processor or the controller.

21 NEW SECTION. **Sec. 202.** PROHIBITIONS. Except as provided in
22 this chapter, it shall be unlawful for a controller or processor to:

23 (1) Process covered data for a covered purpose unless:

24 (a) The controller or processor provides the consumer with a
25 privacy notice as required in section 207 of this act prior to or at
26 the time of such processing; and

27 (b) The consumer provides consent for such processing;

28 (2) Disclose any covered data processed for a covered purpose to
29 federal, state, or local law enforcement;

30 (3) Sell any covered data processed for a covered purpose; or

31 (4) Share any covered data processed for a covered purpose with
32 another controller, processor, or third party unless such sharing is

1 governed by contract pursuant to section 206 of this act and is
2 disclosed to a consumer in the notice required in section 207 of
3 this act.

4 NEW SECTION. **Sec. 203.** CONSUMER RIGHTS. (1) A consumer has the
5 right to opt-out of the processing of covered data concerning the
6 consumer for a covered purpose.

7 (2) A consumer has the right to confirm whether or not a
8 controller is processing covered data concerning the consumer for a
9 covered purpose and access such covered data.

10 (3) A consumer has the right to request correction of inaccurate
11 covered data concerning the consumer processed for a covered
12 purpose.

13 (4) A consumer has the right to request deletion of covered data
14 concerning the consumer processed for a covered purpose.

15 NEW SECTION. **Sec. 204.** EXERCISING CONSUMER RIGHTS. (1) A
16 consumer may exercise the rights set forth in section 203 of this
17 act by submitting a request, at any time, to a controller specifying
18 which rights the consumer wishes to exercise.

19 (2) In the case of processing covered data concerning a known
20 child, the parent or legal guardian of the known child shall
21 exercise the rights of this chapter on the child's behalf.

22 (3) In the case of processing personal data concerning a
23 consumer subject to guardianship, conservatorship, or other
24 protective arrangement under chapter 11.88 RCW, chapter 11.92 RCW,
25 or chapter 11.130 RCW, the guardian or the conservator of the
26 consumer shall exercise the rights of this chapter on the consumer's
27 behalf.

28

29 NEW SECTION. **Sec. 205.** RESPONDING TO REQUESTS. (1) Except as
30 provided in this chapter, controllers that process covered data for
31 a covered purpose must comply with a request to exercise the rights
32 pursuant to section 203 of this act.

1 (2)(a) Controllers must provide one or more secure and reliable
2 means for consumers to submit a request to exercise their rights
3 under this chapter. Such means shall take into account the ways in
4 which consumers interact with the controller and the need for secure
5 and reliable communication of such requests.

6 (b) Controllers shall not require a consumer to create a new
7 account in order to exercise a right, but a controller may require a
8 consumer to use an existing account to exercise the consumer's
9 rights under this chapter.

10 (3)(a) A controller must inform a consumer of any action taken
11 on a request under section 204 of this act without undue delay and
12 in any event within forty-five days of receipt of the request. That
13 period may be extended once by forty-five additional days where
14 reasonably necessary, taking into account the complexity and number
15 of the requests. The controller must inform the consumer of any such
16 extension within forty-five days of receipt of the request, together
17 with the reasons for the delay.

18 (b) If a controller does not take action on the request of a
19 consumer, the controller must inform the consumer without undue
20 delay and at the latest within forty-five days of receipt of the
21 request of the reasons for not taking action and instructions for
22 how to appeal the decision with the controller as described in
23 subsection (4) of this section.

24 (c) Information provided under this section must be provided by
25 the controller free of charge, up to twice annually to the consumer.
26 Where requests from a consumer are manifestly unfounded or
27 excessive, in particular because of their repetitive character, the
28 controller may either: (i) Charge a reasonable fee to cover the
29 administrative costs of complying with the request, or (ii) refuse
30 to act on the request. The controller bears the burden of
31 demonstrating the manifestly unfounded or excessive character of the
32 request.

1 (d) A controller is not required to comply with a request to
2 exercise any of the rights under section 203 of this act if the
3 controller is unable to authenticate the request using commercially
4 reasonable efforts. In such cases, the controller may request the
5 provision of additional information reasonably necessary to
6 authenticate the request.

7 (4)(a) Controllers must establish an internal process whereby
8 consumers may appeal a refusal to take action on a request to
9 exercise any of the rights section 203 of this act within a
10 reasonable period of time after the consumer's receipt of the notice
11 sent by the controller under subsection (3)(b) of this section.

12 (b) The appeal process must be conspicuously available and as
13 easy to use as the process for submitting such requests under this
14 section.

15 (c) Within thirty days of receipt of an appeal, a controller
16 must inform the consumer of any action taken or not taken in
17 response to the appeal, along with a written explanation of the
18 reasons in support thereof. That period may be extended by sixty
19 additional days where reasonably necessary, taking into account the
20 complexity and number of the requests serving as the basis for the
21 appeal. The controller must inform the consumer of any such
22 extension within thirty days of receipt of the appeal, together with
23 the reasons for the delay. The controller must also provide the
24 consumer with an email address or other online mechanism through
25 which the consumer may submit the appeal, along with any action
26 taken or not taken by the controller in response to the appeal and
27 the controller's written explanation of the reasons in support
28 thereof, to the attorney general.

29 (d) When informing a consumer of any action taken or not taken
30 in response to an appeal pursuant to (c) of this subsection, the
31 controller must clearly and prominently ask the consumer whether the
32 consumer consents to having the controller submit the appeal, along
33 with any action taken or not taken by the controller in response to

1 the appeal and must, upon request, provide the controller's written
2 explanation of the reasons in support thereof, to the attorney
3 general. If the consumer provides such consent, the controller must
4 submit such information to the attorney general.

5 NEW SECTION. **Sec. 206.** RESPONSIBILITY ACCORDING TO ROLE. (1)
6 Controllers and processors are responsible for meeting their
7 respective obligations established under this chapter.

8 (2) Processors are responsible under this chapter for adhering
9 to the instructions of the controller and assisting the controller
10 to meet its obligations under this chapter. Such assistance shall
11 include the following:

12 (a) The processor shall assist the controller by appropriate
13 technical and organizational measures, insofar as this is possible,
14 for the fulfillment of the controller's obligation to respond to
15 consumer requests to exercise their rights pursuant to section 203
16 of this act; and

17 (b) The processor shall assist the controller in meeting the
18 controller's obligations in relation to the security of processing
19 the covered data and in relation to the notification of a breach of
20 the security of the system pursuant to RCW 19.255.010.

21 (3) Notwithstanding the instructions of the controller, a
22 processor shall:

23 (a) Implement and maintain reasonable security procedures and
24 practices to protect covered data;

25 (b) Ensure that each person processing the covered data is
26 subject to a duty of confidentiality with respect to the data; and

27 (c) Engage a subcontractor only after providing the controller
28 with an opportunity to object and pursuant to a written contract in
29 accordance with subsection (5) of this section that requires the
30 subcontractor to meet the obligations of the processor with respect
31 to the covered data.

1 (4) Processing by a processor shall be governed by a contract
2 between the controller and the processor that is binding on both
3 parties and that sets out the processing instructions to which the
4 processor is bound, including the nature and purpose of the
5 processing, the type of data subject to the processing, the duration
6 of the processing, and the obligations and rights of both parties.
7 In addition, the contract shall include the requirements imposed by
8 this subsection and subsection (3) of this section, as well as the
9 following requirements:

10 (a) At the choice of the controller, the processor shall delete
11 or return all covered data to the controller as requested at the end
12 of the provision of services, unless retention of the covered data
13 is required by law;

14 (b)(i) The processor shall make available to the controller all
15 information necessary to demonstrate compliance with the obligations
16 in this chapter; and (ii) the processor shall allow for, and
17 contribute to, reasonable audits and inspections by the controller
18 or the controller's designated auditor; alternatively, the processor
19 may, with the controller's consent, arrange for a qualified and
20 independent auditor to conduct, at least annually and at the
21 processor's expense, an audit of the processor's policies and
22 technical and organizational measures in support of the obligations
23 under this chapter using an appropriate and accepted control
24 standard or framework and audit procedure for such audits as
25 applicable, and shall provide a report of such audit to the
26 controller upon request.

27 (5) In no event shall any contract relieve a controller or a
28 processor from the liabilities imposed on them by virtue of its role
29 in the processing relationship as defined by this chapter.

30 (6) Determining whether a person is acting as a controller or
31 processor with respect to a specific processing of data is a fact-
32 based determination that depends upon the context in which personal
33 data are to be processed. A person that is not limited in its

1 processing of covered data pursuant to a controller's instructions,
2 or that fails to adhere to such instructions, is a controller and
3 not a processor with respect to processing of covered data for a
4 covered purpose. A processor that continues to adhere to a
5 controller's instructions with respect to processing of covered data
6 for a covered purpose remains a processor. If a processor begins,
7 alone or jointly with others, determining the purposes and means of
8 the processing of covered data for a covered purpose, it is a
9 controller with respect to such processing.

10

11 NEW SECTION. **Sec. 207.** RESPONSIBILITIES OF CONTROLLERS. (1)

12 *Transparency.* Controllers that process covered data for a covered
13 purpose must provide consumers with a clear and conspicuous privacy
14 notice that includes, at a minimum:

15 (a) How a consumer may exercise the rights contained in section
16 203 of this act, including how a consumer may appeal a controller's
17 action with regard to the consumer's request;

18 (b) The categories of covered data processed by the controller;

19 (c) The purposes for which the categories of covered data are
20 processed;

21 (d) The categories of covered data that the controller shares
22 with third parties, if any; and

23 (e) The categories of third parties, if any, with whom the
24 controller shares covered data.

25 (2) *Purpose Specification.* A controller's collection of covered
26 data must be limited to what is reasonably necessary in relation to
27 the covered purposes for which such data are processed.

28 (3) *Data minimization.* A controller's collection of covered data
29 must be adequate, relevant, and limited to what is reasonably
30 necessary in relation to the covered purpose for which such data are
31 processed.

32 (4) *Avoid secondary use.* Except as provided in this chapter, a
33 controller may not process covered data for purposes that are not

1 reasonably necessary to, or compatible with, the covered purposes
2 for which such personal data are processed unless the controller
3 obtains the consumer's consent. Controllers shall not process
4 covered data or deidentified data that was processed for a covered
5 purpose for purposes of marketing, developing new products or
6 services, or engaging in commercial product or market research.

7 (5) *Security*. A controller shall establish, implement, and
8 maintain reasonable administrative, technical, and physical data
9 security practices to protect the confidentiality, integrity, and
10 accessibility of covered data. Such data security practices shall be
11 appropriate to the volume and nature of the personal data at issue.

12 (6) *Retention*. A controller must delete or deidentify all
13 covered data processed for a covered purpose when such data is no
14 longer being used for such covered purpose.

15 (7) *Nondiscrimination*. A controller shall not process personal
16 data on the basis of a consumer's or a class of consumers' actual or
17 perceived race, color, ethnicity, religion, national origin, sex,
18 gender, gender identity, sexual orientation, familial status, lawful
19 source of income, or disability, in a manner that unlawfully
20 discriminates against the consumer or class of consumers with
21 respect to the offering or provision of (a) housing, (b) employment,
22 (c) credit, (d) education, or (e) the goods, services, facilities,
23 privileges, advantages, or accommodations of any place of public
24 accommodation.

25 (8) *Nonwaiver of consumer rights*. Any provision of a contract or
26 agreement of any kind that purports to waive or limit in any way a
27 consumer's rights under this chapter shall be deemed contrary to
28 public policy and shall be void and unenforceable.

29

30 NEW SECTION. **Sec. 207.** LIMITATIONS AND APPLICABILITY. (1) The
31 obligations imposed on controllers or processors under this chapter
32 do not restrict a controller's or processor's ability to:

1 (a) Comply with federal, state, or local laws, rules, or
2 regulations; or

3 (b) Process deidentified information to engage in public or
4 peer-reviewed scientific, historical, or statistical research in the
5 public interest that adheres to all other applicable ethics and
6 privacy laws as long as such processing is disclosed to the
7 individual in the notice required under section 204 of this act.

8 (2) Covered data that are processed by a controller pursuant to
9 this section must not be processed for any purpose other than those
10 expressly listed in this section. Covered data that are processed by
11 a controller pursuant to this section may be processed solely to the
12 extent that such processing is: (i) Necessary, reasonable, and
13 proportionate to the purposes listed in this section; and (ii)
14 adequate, relevant, and limited to what is necessary in relation to
15 the specific purpose or purposes listed in this section.

16 Furthermore, covered data that are collected, used, or retained
17 pursuant to subsection (2) of this section must, insofar as
18 possible, taking into account the nature and purpose or purposes of
19 such collection, use, or retention, be subjected to reasonable
20 administrative, technical, and physical measures to protect the
21 confidentiality, integrity, and accessibility of the covered data,
22 and to reduce reasonably foreseeable risks of harm to consumers
23 relating to such collection, use, or retention of covered data.

24 (3) If a controller processes covered data pursuant to an
25 exemption in subsection (1) of this section, the controller bears
26 the burden of demonstrating that such processing qualifies for the
27 exemption and complies with the requirements in subsection (2) of
28 this section.

29 (4) Processing covered data solely for the purposes expressly
30 identified in subsection (1) of this section does not, by itself,
31 make an entity a controller with respect to such processing.

1 NEW SECTION. **Sec. 209.** LIABILITY. (1) Any violation of this
2 chapter shall not serve as the basis for, or be subject to, a
3 private right of action under this chapter or under any other law.
4 This does not relieve any party from any duties or obligations
5 imposed, or to alter any independent rights that consumers have
6 under other laws, chapter 19.86 RCW, the Washington state
7 Constitution, or the United States Constitution.

8 (2) Where more than one controller or processor, or both a
9 controller and a processor, involved in the same processing, is in
10 violation of this chapter, the liability must be allocated among the
11 parties according to principles of comparative fault.

12 NEW SECTION. **Sec. 210.** ENFORCEMENT. (1) The legislature finds
13 that the practices covered by this chapter are matters vitally
14 affecting the public interest for the purpose of applying the
15 consumer protection act, chapter 19.86 RCW. A violation of this
16 chapter is not reasonable in relation to the development and
17 preservation of business and is an unfair or deceptive act in trade
18 or commerce and an unfair method of competition for the purpose of
19 applying the consumer protection act, chapter 19.86 RCW.

20 (2) This chapter may be enforced solely by the attorney general
21 under the consumer protection act, chapter 19.86 RCW.

22 (3) Prior to initiating any action under this act, the attorney
23 general must provide a controller thirty days' written notice
24 identifying the specific provisions of this title the attorney
25 general, on behalf of a consumer, alleges have been or are being
26 violated. In the event a cure is possible, if within the thirty days
27 the controller cures the noticed violation and provides the consumer
28 an express written statement that the violations have been cured and
29 that no further violations shall occur, no action for statutory
30 damages may be initiated against the controller. If a controller
31 continues to violate this title in breach of the express written
32 statement provided to the consumer under this subsection, the

1 attorney general may initiate an action and seek damages of up to
2 seven thousand and five hundred dollars for each violation under
3 this act.

4 (4) All receipts from the imposition of civil penalties under
5 this chapter must be deposited into the consumer privacy account
6 established in section 113 of this act.

7 NEW SECTION. **Sec. 211.** PREEMPTION. (1) Except as provided in
8 this section, this chapter supersedes and preempts laws, ordinances,
9 regulations, or the equivalent adopted by any local entity regarding
10 the processing of covered data for a covered purpose by controllers
11 or processors.

12 (2) Laws, ordinances, or regulations regarding the processing
13 covered data for a covered purpose by controllers or processors that
14 are adopted by any local entity prior to July 1, 2020, are not
15 superseded or preempted.

16 **PART 3**

17 **Data Privacy Regarding Public Health Emergency - Public Sector**

18 NEW SECTION. **Sec. 301.** The definitions in this section apply
19 throughout this chapter unless the context clearly requires
20 otherwise.

21 (1) "Consent" means a clear affirmative act signifying a freely
22 given, specific, informed, and unambiguous indication of an
23 individual's agreement to the processing of covered data relating to
24 the individual, such as by a written statement, including by
25 electronic means, or other clear affirmative action.

26 (2) "Controller" means the local government, state agency, or
27 institutions of higher education which, alone or jointly with
28 others, determines the purposes and means of the processing of
29 covered data.

1 (3) "Covered data" includes personal data and one or more of the
2 following: specific geolocation data, proximity data, or personal
3 health data.

4 (4) "Covered purpose" means processing of covered data
5 concerning an individual for the purposes of detecting symptoms of
6 an infectious disease, enabling the tracking of an individual's
7 contacts with other individuals, or with specific locations to
8 identify in an automated fashion whom individuals have come into
9 contact with, or digitally notifying, in an automated manner, an
10 individual who may have become exposed to an infectious disease, or
11 other similar purposes directly related to a state of emergency
12 declared by the governor pursuant to RCW 43.06.010 and any
13 restrictions imposed under the state of emergency declared by the
14 governor pursuant to RCW 43.06.200 through 43.06.270.

15 (5) (a) "Deidentified data" means data that cannot reasonably be
16 used to infer information about, or otherwise be linked to, an
17 identified or identifiable natural person, or a device linked to
18 such person, provided that the controller that possesses the data:
19 (i) Takes reasonable measures to ensure that the data cannot be
20 associated with a natural person; (ii) publicly commits to maintain
21 and use the data only in a deidentified fashion and not attempt to
22 reidentify the data; and (iii), except as provided in subsection (b)
23 of this subsection, contractually obligates any recipients of the
24 information to comply with all provisions of this subsection. (b)
25 For purposes of this subsection, the obligations imposed under (iii)
26 of this subsection shall not apply when a controller discloses
27 deidentified data to the public pursuant to chapter 42.56 RCW or
28 other state disclosure laws.

29 (6) "Delete" means to remove or destroy information such that it
30 is not maintained in human or machine-readable form and cannot be
31 retrieved or utilized in the course of business.

32 (7) "Identified or identifiable natural person" means an
33 individual who can be readily identified, directly or indirectly.

1 (8) "Individual" means a natural person who is a Washington
2 resident acting only in an individual or household context. It does
3 not include a natural person acting in a commercial or employment
4 context.

5 (9) "Institutions of higher education" has the same meaning as
6 in RCW 28B.92.030.

7 (10) "Local government" has the same meaning as in RCW
8 39.46.020.

9 (11) "Local health departments" has the same meaning as in RCW
10 70.05.010.

11 (12)(a) "Personal data" means any information that is linked or
12 reasonably linkable or describes or is reasonably capable of being
13 associated to an identified or identifiable natural person.
14 "Personal data" does not include deidentified data or publicly
15 available information.

16 (b) For purposes of this subsection, "publicly available
17 information" means information that is lawfully made available from
18 federal, state, or local government records.

19 (13) "Personal health data" means information relating to the
20 past, present, or future diagnosis or treatment of an individual
21 regarding an infectious disease.

22 (14) (a) "Process," "processed," or "processing" means any
23 operation or set of operations which are performed on covered data
24 or on sets of covered data by automated means, such as the
25 collection, use, storage, disclosure, analysis, deletion, or
26 modification of covered data.

27 (b) Processing does not include means such as recognized
28 investigatory measures intended to gather information to facilitate
29 investigations including but not limited to traditional in-person,
30 email, or telephonic activities used as of the effective date of
31 this act by the department of health, created under chapter 43.70
32 RCW, or local health departments to provide for the control and
33 prevention of any dangerous, contagious, or infectious disease.

1 (15) "Processor" means a natural or legal person, local
2 government, state agency, or institutions of higher education that
3 processes covered data on behalf of a controller.

4 (16) "Proximity data" means technologically derived information
5 that identifies past or present proximity of one individual to
6 another, or the proximity of natural persons to other locations or
7 objects.

8 (17) "Secure" means encrypted in a manner that meets or exceeds
9 the national institute of standards and technology standard or is
10 otherwise modified so that the covered data is rendered unreadable,
11 unusable, or undecipherable by an unauthorized person.

12 (18) "Sell" means the exchange of covered data for monetary or
13 other valuable consideration by the controller to a third party. For
14 the purposes of this subsection, "sell" does not include the
15 recovery of fees by a controller.

16 (19) "Specific geolocation data" means information derived from
17 technology, including, but not limited to, global positioning system
18 level latitude and longitude coordinates or other mechanisms, that
19 directly identifies the specific location of a natural person with
20 the precision and accuracy below one thousand seven hundred fifty
21 feet. Specific geolocation data excludes the content of
22 communications.

23 (20) "State agency" has the same meaning as in RCW 43.105.020.

24 (21) "Third party" means a natural or legal person, public
25 authority, agency, or body other than the individual, controller,
26 processor, or an affiliate of the processor or the controller.

27 NEW SECTION. **Sec. 302.** PROHIBITIONS. Except as provided in
28 this chapter, it shall be unlawful for a controller or processor to:

29 (1) Process covered data for a covered purpose unless:

30 (a) The controller or processor provides the individual with a
31 privacy notice prior to or at the time of such processing; and

32 (b) The individual provides consent for such processing;

1 (2) Disclose any covered data processed for a covered purpose to
2 federal, state, or local law enforcement;

3 (3) Sell any covered data processed for a covered purpose; or

4 (4) Share any covered data processed for a covered purpose with
5 another controller, processor, or third party unless such sharing is
6 governed by contract or data sharing agreement as prescribed in
7 section 303 of this act and is disclosed to an individual in the
8 notice required in section 304 of this act.

9
10 NEW SECTION. **Sec. 303.** RESPONSIBILITY ACCORDING TO ROLE. (1)

11 Controllers and processors are responsible for meeting their
12 respective obligations established under this chapter.

13 (2) Processors are responsible under this chapter for adhering
14 to the instructions of the controller and assisting the controller
15 to meet its obligations under this chapter. Such assistance shall
16 include the processor assisting the controller in meeting the
17 controller's obligations in relation to the security of processing
18 the covered data and in relation to the notification of a breach of
19 the security of the system pursuant to RCW 42.56.590.

20 (3) Notwithstanding the instructions of the controller, a
21 processor shall:

22 (a) Implement and maintain reasonable security procedures and
23 practices to protect covered data;

24 (b) Ensure that each person processing the covered data is
25 subject to a duty of confidentiality with respect to the data; and

26 (c) Engage a subcontractor only after providing the controller
27 with an opportunity to object and pursuant to a written contract in
28 accordance with subsection (5) of this section that requires the
29 subcontractor to meet the obligations of the processor with respect
30 to the covered data.

31 (4) Processing by a processor shall be governed by a contract or
32 data sharing agreement between the controller and the processor that
33 is binding on both parties and that sets out the processing

1 instructions to which the processor is bound, including the nature
2 and purpose of the processing, the type of data subject to the
3 processing, the duration of the processing, and the obligations and
4 rights of both parties. In addition, the contract or data sharing
5 agreement shall include the requirements imposed by this subsection
6 and subsection (3) of this section, as well as the following
7 requirements:

8 (a) At the choice of the controller, the processor shall delete
9 or return all covered data to the controller as requested at the end
10 of the provision of services, unless retention of the covered data
11 is required by law;

12 (b)(i) The processor shall make available to the controller all
13 information necessary to demonstrate compliance with the obligations
14 in this chapter; and (ii) the processor shall allow for, and
15 contribute to, reasonable audits and inspections by the controller
16 or the controller's designated auditor; alternatively, the processor
17 may, with the controller's consent, arrange for a qualified and
18 independent auditor to conduct, at least annually and at the
19 processor's expense, an audit of the processor's policies and
20 technical and organizational measures in support of the obligations
21 under this chapter using an appropriate and accepted control
22 standard or framework and audit procedure for such audits as
23 applicable, and shall provide a report of such audit to the
24 controller upon request.

25 (5) In no event shall any contract or data sharing agreement
26 relieve a controller or a processor from the liabilities imposed on
27 them by virtue of its role in the processing relationship as defined
28 by this chapter.

29 (6) Determining whether a person is acting as a controller or
30 processor with respect to a specific processing of data is a fact-
31 based determination that depends upon the context in which covered
32 data are to be processed. A person that is not limited in its
33 processing of covered data pursuant to a controller's instructions,

1 or that fails to adhere to such instructions, is a controller and
2 not a processor with respect to processing of covered data for a
3 covered purpose. A processor that continues to adhere to a
4 controller's instructions with respect to processing of covered data
5 for a covered purpose remains a processor. If a processor begins,
6 alone or jointly with others, determining the purposes and means of
7 the processing of covered data for a covered purpose, it is a
8 controller with respect to such processing.

9 NEW SECTION. **Sec. 304.** RESPONSIBILITIES OF CONTROLLERS. (1)
10 *Transparency.* Controllers that process covered data for a covered
11 purpose must provide individuals with a clear and conspicuous
12 privacy notice that includes, at a minimum:

13 (a) The categories of covered data processed by the controller;

14 (b) The purposes for which the categories of covered data are
15 processed;

16 (c) The categories of covered data that the controller shares
17 with third parties, if any; and

18 (d) The categories of third parties, if any, with whom the
19 controller shares covered data.

20 (2) *Purpose Specification.* A controller's collection of covered
21 data must be limited to what is reasonably necessary in relation to
22 the covered purpose for which such data are processed.

23 (3) *Data minimization.* A controller's collection of covered data
24 must be adequate, relevant, and limited to what is reasonably
25 necessary in relation to the covered purposes for which such data
26 are processed.

27 (4) *Avoid secondary use.* Except as provided in this chapter, a
28 controller may not process covered data for purposes that are not
29 reasonably necessary to, or compatible with, the covered purposes
30 for which such covered data are processed unless the controller
31 obtains the individual's consent. Controllers shall not process
32 covered data or deidentified data that was processed for a covered

1 purpose for purposes of marketing, developing new products or
2 services, or engaging in commercial product or market research.

3 (5) *Security*. A controller shall establish, implement, and
4 maintain reasonable administrative, technical, and physical data
5 security practices to protect the confidentiality, integrity, and
6 accessibility of covered data. Such data security practices shall be
7 appropriate to the volume and nature of the personal data at issue.

8 (6) *Retention*. A controller must delete or deidentify all
9 covered data processed for a covered purpose when such data is no
10 longer being used for a covered purpose and has met records
11 retention as required by federal or state law.

12 (7) *Nondiscrimination*. A controller shall not process covered
13 data on the basis of an individual's or a class of individuals'
14 actual or perceived race, color, ethnicity, religion, national
15 origin, sex, gender, gender identity, sexual orientation, familial
16 status, lawful source of income, or disability, in a manner that
17 unlawfully discriminates against the individual or class of
18 individuals with respect to the offering or provision of (a)
19 housing, (b) employment, (c) credit, (d) education, or (e) the
20 goods, services, facilities, privileges, advantages, or
21 accommodations of any place of public accommodation.

22 NEW SECTION. **Sec. 305.** LIMITATIONS AND APPLICABILITY. (1) The
23 obligations imposed on controllers or processors under this chapter
24 do not restrict a controller's or processor's ability to:

25 (a) Comply with federal, state, or local laws, rules, or
26 regulations; or

27 (b) Process deidentified information to engage in public or
28 peer-reviewed scientific, historical, or statistical research in the
29 public interest that adheres to all other applicable ethics and
30 privacy laws as long as such processing is disclosed to the
31 individual in the notice required under section 304 of this act.

1 (2) Covered data that are processed by a controller pursuant to
2 this section must not be processed for any purpose other than those
3 expressly listed in this section. Covered data that are processed by
4 a controller pursuant to this section may be processed solely to the
5 extent that such processing is: (i) Necessary, reasonable, and
6 proportionate to the purposes listed in this section; and (ii)
7 adequate, relevant, and limited to what is necessary in relation to
8 the specific purpose or purposes listed in this section.

9 Furthermore, covered data that are collected, used, or retained
10 pursuant to subsection (2) of this section must, insofar as
11 possible, taking into account the nature and purpose or purposes of
12 such collection, use, or retention, be subjected to reasonable
13 administrative, technical, and physical measures to protect the
14 confidentiality, integrity, and accessibility of the covered data,
15 and to reduce reasonably foreseeable risks of harm to individuals
16 relating to such collection, use, or retention of covered data.

17 (3) If a controller processes covered data pursuant to an
18 exemption in subsection (1) of this section, the controller bears
19 the burden of demonstrating that such processing qualifies for the
20 exemption and complies with the requirements in subsection (2) of
21 this section.

22 (4) Processing covered data solely for the purposes expressly
23 identified in subsection (1)(a) and (b) of this section does not, by
24 itself, make an entity a controller with respect to such processing.

25 NEW SECTION. **Sec. 306.** LIABILITY. Where more than one
26 controller or processor, or both a controller and a processor,
27 involved in the same processing, is in violation of this chapter,
28 the liability must be allocated among the parties according to
29 principles of comparative fault.

30 NEW SECTION. **Sec. 307.** ENFORCEMENT. (1) Any waiver of the
31 provisions of this chapter is contrary to public policy, and is void
32 and unenforceable.

1 (2)(a) Any individual injured by a violation of this chapter may
2 institute a civil action to recover damages.

3 (b) Any controller that violates, proposes to violate, or has
4 violated this chapter may be enjoined.

5 (c) The rights and remedies available under this chapter are
6 cumulative to each other and to any other rights and remedies
7 available under law.

8

9

PART 4

10

11 NEW SECTION. **Sec. 401.** Sections 101 through 116 and sections
12 201 through 211 of this act constitute new chapters in Title 19 RCW.

13 NEW SECTION. **Sec. 402.** Sections 301 through 307 of this act
14 constitute a new chapter in Title 43 RCW.

15 NEW SECTION. **Sec. 403.** Except for sections 1, 2, and 101
16 through 117, this act is necessary for the immediate preservation of
17 the public peace, health, or safety, or support of the state
18 government and its existing public institutions, and takes effect
19 immediately.
20

21 NEW SECTION. **Sec. 404.** Sections 1, 2, and 101 through 117 of
22 this act take effect one hundred and twenty days after enactment.
23

24

25

--- END ---